REMARKS

The Examiner is respectfully requested to reconsider his rejection of claims 1 - 4, 10 and 11 under 35 U.S.C. §103(a) as being unpatentable over United States Patent 6,088,450 to Davis, et al. in view of United States Patent 6,898,711 B1 to Bauman, et al.

The Examiner is respectfully requested to review his interpretation of the Davis et al. reference and the manner in which he has applied same to the claims in the instant application. The Examiner asserts that each and every element claimed by Applicants is found in the Davis, et al. reference. The Examiner in his rejections in the above-noted Office Action cites the specific language found in Applicants' claims and bases his anticipation rejections on excerpts from the Davis reference which in fact do not support his assertions.

The Examiner's rejections are quoted *verbatim* and listed *seriatem,* with Applicants' responses to the specific rejection presented immediately thereafter.

The Examiner asserts: "As to claim 1, Davis et al discloses a method for setting basic means of access for operation of devices which the operation is controllable by electronic means, comprising: the device comprising mobile phones, small computer-controlled consumer devices with relatively low level of computing power, computers, motor vehicles, control terminals for industrial processes, all of which devices may require authentication prior to operation [column 3 line 52 to column 4 line 11];

Applicants respectfully respond that the Davis invention is directly related to wireless devices (only) and his invention is targeted on basic level authentication (user can access the device or not access it) and solving the additional hurdles that a wireless connection provides. The present invention does not limit the means of how the connection is established between the token and the device. In the instant invention, Applicants focus on a smart card which could have a physical

or a wireless/contactless connection to the reader. This is a major distinction which is defined in the claims.

The Examiner continues with his rejection referring to the next portion of Claim 1:
"establishment of a link between a personal authentication system supplied with encryption data and a logic system able to control an electronic device control [column 4, lines 12-19];

Respectfully, column 4, lines 15 -19 have been misinterpreted by the Examiner. Column 4, lines 15 -19 clearly states: ".. the user is granted access to the contents of the personal computer as well as its networked resources." This statement means that there is only <u>one</u> level of authentication (access yes/no). The present invention solves the need to have different levels of access where in claim 1, lines 12- 15 Applicants claim: *"Enabling (150) of the means of access predetermined for the authentication system (16) dependent on the result of the check")*

The Examiner continues with his rejection referring to the next portion of Claim 1:
"assignment of predetermined means of access to the electronic device control associated with the authentication system the predetermined means providing access to the physical hardware resources and access to different functions, based on the privileges of the user who identified himself to the system, the software function evaluates a security token and is running on top of te physical hardware [column 5 line 50 to column 6 line 50];"

Again, most respectfully, column 5, line 50 to column 6 line 50 have been misinterpreted by the Examiner. This comment in the rejection raises an inference that the Examiner has not understood a main point of the invention The excerpt cited at column 5 line 50 to column 6 line 50 make clear that Davis is only providing authentication at one level (access Yes/No). As described by Applicants in their invention disclosure, they provide different levels of authentication, based on the security token and the need the user/admin/service personnel has. Thus the present invention is not limited to a single level of authentication.

In the Davis patent, when considering "*access*," there is only one level of access. An important distinguishing key to the present invention is that there are different levels of access to differentiate the different levels of authentication that persons with different roles may need. The Examiner is referred to page 6 of the specification. The different levels are mentioned on page 6. At that location, there is a disclosure of the system being open to progressive hierarchies of access rights to the device, for example, by the production of a Master SmartCard which can be issued to customers' service personnel in order to configure large numbers of individual devices. Further, on page 6: "Applying the method in accordance with the invention, and based on the stipulation that a single SmartCard is to be able to configure any number of devices but that only a Master SmartCard or a personal SmartCard can be used to shut down and/or startup/restart the devices, a device manufacturer may do the following..." Applicants differentiate between a single (standard) smart card and a Master Smart Card.

The different levels are mentioned in the portion of Claim 1 that reads: "...assignment of predetermined means of access to the device associated with the authentication system said predetermined means of access being dependent upon the level of authorization that is set in said personal authorization system."

The Examiner continues with his rejection referring to the next portion of Claim 1:
"enabling of the means for access predetermined for the authetication system dependent on the result of the check [column 5 line 50 to column 6 line 50];"

As noted above, "column 5 line 50 to column 6 line 50 make really clear that Davis is only providing authentication at one level (access Yes/No). As described in the invention , Applicants provide different levels of authentication, based on the security token and the need the user/admin/service personnel has. There is no differentiation in Davis based on the role of the user.

The Examiner then states that "Bauman, et al. teaches providing means of no access or full access and allows more finely defined levels of access as defined in a user profile (citation omitted).

Bauman focuses on a multi-process environment (See Abstract: "A multi-process environment...") and distributed processing systems (Column 1, lines 12 - 13). The environments of the present invention are not multi-process environments, but are simple devices with one process running at a time.

In Column 5, lines 35 - 36, Bauman discloses a client/server system within a three-tier environment. The reference states there: "One particular client/server system within a multitier paradigm." Further on the the disclosure, Bauman states: "A user authentication methodology according to the present invention may be implemented in any multiple process environment..." (Column 5, lines 57 - 59)

In view of Bauman, Applicants have amended Claim 1 to read that the invention is targeting "single process/tasking systems" since Bauman is directed to a "multi-process environment(s)." There is no suggestion to combine the references with respect to the manner in which Claim 1 has been amended as Applicants are claiming a single system and Bauman is disclosing a multi tier system.

As to claim 2, Davis et al. discloses that the basic means of access of functions of the device comprise at least one of the following means: disable operation of the devices, enable operation of the devices, or enable configuration of the devices [column 5 line 50 to column 6 line 50].

At the location cited in the reference which forms the basis for the anticipation rejection, [i.e., column 5 line 50 to column 6 line 50] Applicants do not find any specific reference to or for a third level of access (like the configuration of the device). Davis consistently only refers to "given access" or "denied access." It is not clear how this should relate to the present invention. Clarification is requested. In addition, for the reasons stated above, the rejection herein using Bauman as embodied in the rejection of independent Claim 1 is improper and thus the rejection of dependent Claim 2 is without proper foundation.

As to claim 3, Davis et al discloses in addition, that the link is made without need for intermediate software layers [column 7, lines 35 - 62].

The Davis disclosure at column 7, lines 35 - 62 relates to having the token itself password protected. Applicants do not understand how this relates to instant Claim 3. In addition, for the reasons stated above, the rejection herein using Bauman as embodied in the rejection of independent Claim 1 is improper and thus the rejection of dependent Claim 3 is without proper foundation.

As to claim 4, Davis et al discloses in addition, the step of reading at least one of the following features embodied with the authentication system: firmware programs, device-specific command sequences for execution of specific device-specific functions, cryptographic keys, cryptographic algorithms, and individual decision making logic [column 5, lines 34-49].

From Applicants review of column 5, lines 34-49, there is no mention of "firmware programs", "individual decision making logic", or "device-specific command sequences for execution of specific device-specific functions." In addition, for the reasons stated above, the rejection herein using Bauman as embodied in the rejection of independent Claim 1 is improper and thus the rejection of Claim 4 is without proper foundation.

As to claim 10, Davis et al discloses program code areas for the execution or preparation for execution of the steps when the program is installed in a computer [column 5, lines 34-49].

Applicants do not read any teaching in Davis at column 5, lines 34-49, that relates to installing a program in a computer.

In addition, with respect to Claim 10, for the reasons stated above, the rejection herein using Bauman as embodied in the rejection of independent Claim 1 is improper and thus the rejection of Claim 10 is without proper foundation.

"As to claim 11, Davis et al discloses a method for setting basic means of access for operation of devices of which the operation is controllable for electronic means, comprising:
the devices comprising computer-controlled consumer devices with relatively low level of computing power, computers, motor vehicles, control terminal for industrial processes, all of which devices may require authentication prior to operation [column 3, lines 52 to column 4 line 11];"

Applicants do not read any teaching at column 3, lines 52 to column 4 line 11 that relates to devices that "*all of which devices may require authentication prior to operation.*"

"establishment of a link between a personal authentication system supplied with encryption data and a logic system able to control an electronic device control [column 4, lines 12-19];..."

In responding to the balance of anticipation rejections asserted by the Examiner of Claim 11, Davis only has Access Yes/No, but no way to provide different levels of access.

In addition, for the reasons stated above, the rejection herein using Bauman as embodied in the rejection of independent Claim 1 is improper and thus the rejection of Claim11 is without proper foundation.

The Examiner is respectfully requested to reconsider his rejection of claims 5 - 9 under 35 U.S.C. §103(a) as being unpatentable over United States Patent 6,088,450 to Davis, et al. and United States Patent 6,898,711 B1 to Bauman, et al. as applied to Claim 1, and further in view of United States Patent 6,415,144 to Findikli, et al.

The Examiner acknowledges in the Official Action that Davis, et al. does not teach the method including configuration of the devices by authorized persons. In addition, for the reasons stated above, the rejection herein using Bauman as embodied in the rejection of independent Claim 1 is improper and thus the rejection of Claim 5 is without proper foundation. Bauman is not relevant. With regard to the further rejection of Claim 5, Findikli, et al. teach download of configuration information, in an insecure way. There is no connection to any security system on the device. There is also no way to personalize/customize the configuration without the mobile phone being registered with a service provider, which may not always be the case for all the devices (like to a ladling phone, or a washing machine).

With respect to claim 5, Davis et al does not teach that the method includes configuration of the devices, by authorized persons. Davis et al does not teach after successful authentication, device-specific configuration data are downloaded into the devices from the authentication system in accordance with the authentication systems or over the network.

The Examiner says that Findikli et al teaches configuration of the devices, by authorized persons [column 1 line 61 to column 2 line 5]. Findikli at column 1 line 61 to column 2 line 5 doesn't mention anything about authorization and/or authorized persons.

The Examiner also asserts that Findikli et al teaches that device-specific configuration data are downloaded into the devices from the authentication system in accordance with the authentication systems or over a network [column 1 line 61 to column 2 line 5]. This assertion is correct, but the Examiner misses a main point of the present invention. Applicants have different level of access, not only "Yes/No", like Davis. There is no mentioning of authorization / access control in Fidikli. The present invention is designed to provide a separate level of

authorization, to service personnel required to re-configure the device. There is no basis to combine these references.

The Examiner contends: "as to claim 6, Davis et al teaches execution setting basic means of access for operations [column 6, line 26-50]. Claim 6 is a dependent claim for a device (12) for execution of the basic means of access. Applicants are not sure how the content of Claim 6 is related to what the Examiner has mentioned. Please provide clarification. In addition, for the reasons stated above, the rejection herein using Bauman as embodied in the rejection of independent Claim 1 is improper and thus the rejection of Claim 6 is without proper foundation.

"As to claim 7, Davis et al teaches authentication of person or a group of people [column 6, lines 26-50].
Applicants do not note any mention of "groups" in Davis at column 6, lines 26-50. Further, with respect to Claim 7, Davis does not teach the access of different groups or people with different roles. In addition, for the reasons stated above, the rejection herein using Bauman as embodied in the rejection of independent Claim 1 is improper and thus the rejection of Claim 7 is without proper foundation.

"As to claim 8, Davis et al teaches that the authentication system is implemented in the form of a Smartcard [column 4, lines 20 - 28].
Applicants do not note any mention of "smart cards"or tokens in Davis at column 4, lines 20 - 28. Applicants detail the usage of the token to provide specific configuration information, which defines constraints for the usage of a particular user. This "constraint" e.g. temporary deactivation, limits the usage of a reduced feature set. This is more than just "authentication". It adds "authorization"patterns. The configuration procedure enables or disables various logic components in the sets depending on the customer's specific requirements. In addition, for the reasons stated above, the rejection herein using Bauman as embodied in the rejection of independent Claim 1 is improper and thus the rejection of Claim 8 is without proper foundation.

As to claim 9, Davis et al teach setting basic means of access for operation of devices of which the operation is controllable by electronic means, including at least one device and an authentication system [column 6, lines 26 - 50]

Claim 9 states that: "said encryption data being stored solely in said authentication system." In the event a public or private key infrastructure is used, the required keys are stored in their entirety, for example, on the smart card as well as on the device. In Applicants' invention, a key may be present on the device and the same key on the smart card, so a challenge/response can be used to authenticate the smart card. In addition, for the reasons stated above, the rejection herein using Bauman as embodied in the rejection of independent Claim 1 is improper and thus the rejection of Claim 9 is without proper foundation.

As to Claims 8 and 9, there is no basis for combining the three references. It was demonstrated above that Davis and Findikli do not describe the inventions that warrant the proposed combination. These references, alone or in combination do not disclose the invention defined in claims 8 and 9. The rejection of the claims using Bauman is without foundation.

Davis, et al. Bauman and Findikli, et al., alone, or in combination, do not disclose or even imply the elements of Claims 5 - 9 of the present invention. In the rejection, the Examiner is selectively picking and choosing individual elements disclosed in the references to the exclusion of what the references as a whole teach to one skilled in the art.

In order to analyze the propriety of the Examiner's rejections in this case, a review of the pertinent applicable law relating to 35 U.S.C. § 103 is warranted. The Examiner has applied the Davis, et al. Bauman and Findikli, et al. references discussed above using selective combinations to render obvious the invention.

The Court of Appeals for the Federal Circuit has set guidelines governing such application of references. These guidelines are, as stated are found in Interconnect Planning Corp. v. Feil, 774 F.2d 1132, 1143, 227 USPQ, 543, 551:

> When prior art references require selective combination by the court to render obvious a subsequent invention, there must be some reason for the combination other than hindsight gleaned from the invention itself.

A representative case relying upon this rule of law is Uniroyal, Inc. v. Rudkin-Wiley Corp., 837 F.2d 1044, 5 USPQ 2d 1434 (Fed. Cir. 1988). The district court in Uniroyal found that a combination of various features from a plurality of prior art references suggested the claimed invention of the patent in suit. The Federal Circuit in its decision found that the district court did not show, however, that there was any teaching or suggestion in any of the references, or in the prior art as a whole, that would lead one with ordinary skill in the art to make the combination. The Federal Circuit opined:

> Something in the prior art as a whole must suggest the desirability, and thus the obviousness, of making the combination. [837 F.2d at 1051, 5 USPQ 2d at 1438, citing Lindemann, 730 F.2d 1452, 221 USPQ 481, 488 (Fed. Cir. 1984).]

The Examiner in his application of the cited references is improperly picking and choosing. The rejections are all a piecemeal construction of the invention. Such piecemeal reconstruction of the prior art patents in light of the instant disclosure is contrary to the requirements of 35 U.S.C. § 103.

> The ever present question in cases within the ambit of 35 U.S.C. § 103 is whether the subject matter as a whole would have been obvious to one of ordinary skill in the art following the teachings of the prior art at the time the invention was made. It is impermissible within the framework of Section 103 to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art. (Emphasis in original) In re Wesslau 147 U.S.P.Q. 391, 393 (CCPA 1965)

This holding succinctly summarizes the Examiner's application of references in this case, because the Examiner did in fact pick and choose so much of the Bauman and Findikli, et al. references with respect to "device specific configuration data" to support the rejection and did not cover completely or

accurately in the Office Action the full scope of what these varied disclosure references fairly suggest to one skilled in the art.

Further, the Federal Circuit has stated that the Patent Office bears the burden of establishing obviousness. It held this burden can only be satisfied by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of the reference.

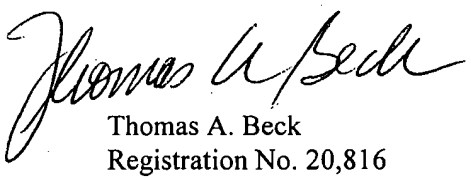
> Obviousness is tested by "what the combined teachings of the references would have suggested to those of ordinary skill in the art." In re Keller, 642 F.2d 413, 425, 208 USPQ 871, 881 (CCPA 1981). But it "cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination." ACS Hosp. Sys., 732 F.2d at 1577, 221 USPQ at 933. [837 F.2d at 1075, 5 USPQ 2d at 1599.]

The Court concluded its discussion of this issue by stating that teachings or references can be combined only if there is some suggestion or incentive to do so.

In the present case, the skilled artisan, viewing the references would not be directed toward Applicants' system. There can reasonably be no system such as Applicants emanating from the Davis, et al., Bauman and Findikli, et al. references as the basic focus of the two references are different. There is no proper basis to combine them.

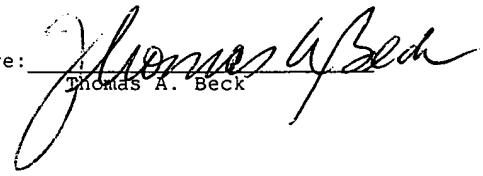
Applicants have attempted in this response to include language limitations to specifically define the invention and to clear up any ambiguities that may have existed in the wording heretofore. Applicants believe that the amended claims are in a form which should result in their allowability. If there are additions which could result in the claims being allowed, Applicants' attorney would be pleased to speak with the Examiner by phone concerning such action at a mutually agreeable time and will cooperate in any way possible.

Respectfully Submitted,



Thomas A. Beck
Registration No. 20,816
26 Rock Ledge Lane
New Milford, CT 06776
(860) 354-0892

I hereby certify that this amendment response is being deposited with the United States Postal Service, in a secure envelope, postage prepaid, on the date indicated below addressed to Commissioner of Patents & Trademarks, Post Office Box 1450, Alexandria, VA 22313-1450

Signature: 
Name: Thomas A. Beck

Date: March 19, 2006

APPENDIX A

1. (Currently amended) A method for setting basic means of access for operation of devices of which the operation is controllable by electronic means, comprising:

said devices comprising mobile phones, small computer-controlled consumer devices with relatively low level of computing power, computers, motor vehicles, control terminals for industrial processes, all of which devices may require authentication prior to operation;

establishment of a link between a personal authentication system supplied with encryption data and a logic system able to control an electronic device control, said encryption data being stored solely in said authentication system, said link between said authentication system and said device being via wired or wireless means;

checking said encryption data in said authentication system prior to operation of said electronic device control;

assignment of predetermined means of access to said electronic device control associated with said authentication system said predetermined means providing access to physical hardware resources and access to different software functions, based on the privileges of the user who identified himself to the system, said software function evaluates a security token and is running on top of said physical hardware, said predetermined means of access being dependent upon the level of authorization that is set in said personal authorization system;

enabling of said predetermined means for access for said authentication system dependent on the result of said check;

said method <u>targeting single process/tasking systems and</u> providing means of no access or full access and allows more finely defined levels of access as defined in a user profile for configuration or maintenance work.

2 . (Previously presented) The method defined in Claim 1, wherein said basic means of access to functions of said device comprise at least one of the following means: disable operation of said devices, enable operation of said devices, or enable configuration of said devices.

3. (Previously presented) The method defined in Claim 2 wherein said link is made without need for intermediate software layers.

4. (Previously presented) The method defined in Claim 3 includes in addition, the step of reading at least one of the following features embodied within said authentication system: firmware programs, device-specific command sequences for execution of specific device-specific functions, cryptographic keys, cryptographic algorithms, and individual decision-making logic.

5. (Previously presented) The method defined in claim 4 which includes configuration of said devices; by authorized persons, wherein after successful authentication, device-specific configuration data are downloaded into said devices from said authentication system in accordance with said authentication systems or over a network.

6. (Previously presented) A device comprising the elements defined in Claim 5 for execution setting basic means of access for operations.

7 . (Previously presented) An authentication system, created for authentication of a person or a group of people, comprising the elements defined in Claim 5.

8. (Previously presented) The authentication system defined in Claim 7 which is implemented in the form of a SmartCard .

9. (Previously presented) A system for setting basic means of access for operation of devices of which the operation is controllable by electronic means, including at least one device and an authentication system as defined in Claim 8.

10. (Previously presented) A computer program, containing program code areas for the execution or preparation for execution of the steps of the method in accordance with Claim 4, when said program is installed in a computer.

11. (Currently Amended) A method for setting basic means of access for operation of devices of which the operation is controllable by electronic means, comprising:

said devices comprising small computer-controlled consumer devices with relatively low level of computing power, computers, motor vehicles, control terminals for industrial processes, all of which devices may require authentication prior to operation;

establishment of a link between a personal authentication system supplied with encryption data and a logic system able to control an electronic device control, said encryption data being stored solely in said authentication system, said link between said authentication system and said device being via wired or wireless means;

checking said encryption data in said authentication system prior to operation of said electronic device control;

assignment of predetermined means of access to said electronic device control associated with said authentication system said predetermined means providing access to physical hardware resources and access to different software functions, based on the privileges of the user who identified himself to the system, said software function evaluates a security token and is running on top of said physical hardware, said predetermined means of access being dependent upon the level of authorization that is set in said personal authorization system;
enabling of said means for access predetermined for said authentication system dependent on the result of said check;

said method <u>targeting single process/tasking systems and</u> providing means of no access or full access and allows more finely defined levels of access as defined in a user profile for configuration or maintenance work.